Our Ref. No. 042390.P7709
Express Mail No.: EL466332415US

UNITED STATES PATENT APPLICATION

FOR

# A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

INVENTORS:

Carl M. Ellison
James A. Sutton

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
(714) 557-3800

# A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

Field

This invention relates to the field of data security. In particular, the invention relates to a platform and method that protects an identity of the platform through creation and use of pseudonyms.

Background

Advances in technology have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (e-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while electronic platforms like computers provide users with convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable for unscrupulous attacks. This vulnerability has substantially hindered the willingness of content providers from providing their content in a downloaded, digital format.

Currently, various mechanisms have been proposed to verify the identity of a platform. This is especially useful to determine if the platform features a "trusted" device; namely, the device is configured to prevent digital content from being copied in a non-encrypted format without authorization. One verification scheme involves the use of a unique serial number assigned to a platform for identification of that platform. Another verification scheme, performed either independently from or cooperatively with the previously described verification scheme, involves the use of a permanent key pair. The permanent key pair includes (i) a unique public key that identifies the platform and (ii) a private key that is permanently stored in memory of the trusted device. The private key is confidential and is not provided outside the trusted device. However, these verification schemes pose a number of disadvantages.

For example, each of these verification schemes is still subject to data aggregation attacks. "Data aggregation" involves the collection and analysis of data transmitted from a platform over a period of time. Thus, the use of platform serial numbers and permanent keys for identification purposes has recently lead to consumer privacy concerns. Also, for both verification mechanisms, a user cannot

easily and reliably control access to and use of the platform identity on a per-use basis.

## BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a block diagram of an illustrative embodiment of a system utilizing the present invention.

Figure 2 is a block diagram of an illustrative embodiment of the trusted logic employed within the first platform of Figure 1.

Figure 3 is a flowchart of an illustrative embodiment describing allocation and use of a pseudonym produced within the first platform of Figure 1.

Figures 4 and 5 are flowcharts of an illustrative embodiment of the production and certification of pseudonyms.

## DETAILED DESCRIPTION

The present invention relates to a platform and method for protecting the identity of the platform through the creation and use of pseudonyms. Herein, certain details are set forth in order to provide a thorough understanding of the present invention. It is apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments other that those illustrated. Well-known circuits and cryptographic techniques are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the following description, terminology is used to discuss certain features of the present invention. For example, a "platform" includes hardware and/or software that process information. Examples of a platform include, but are not limited or restricted to any of the following: a computer (e.g., desktop, a laptop, a hand-held, a server, a workstation, etc.); data transmission equipment (e.g., a router, switch, facsimile machine, etc.), wireless equipment (e.g., cellular base station, telephone handset, etc.); or television set-top box. "Software" includes code that, when executed, performs a certain function. "Information" is defined as one or more bits of data, address, and/or control.

With respect to cryptographic functionality, a "cryptographic operation" is an operation performed for additional security on information. These operations may include encryption, decryption, hash computations, and the like. In certain cases, the cryptographic operation requires the use of a key, which is a series of

bits. For asymmetric key cryptography, a device is associated with unique, permanent key pair that includes a public key and a private key.

In addition, asymmetric key cryptography normally utilizes a root certificate. A "root certificate" is a public key at the origination of a digital certificate chain and provides a starting point for all subsequent digital certificates. In general, a "digital certificate" includes information used to authenticate a sender of information. For example, in accordance with CCITT Recommendation X.509: The Directory - Authentication Framework (1988), a digital certificate may include information (e.g., a key) concerning a person or entity being certified, namely encrypted using the private key of a certification authority. Examples of a "certification authority" include an original equipment manufacturer (OEM), a software vendor, a trade association, a governmental entity, a bank or any other trusted business or person. A "digital certificate chain" includes an ordered sequence of two or more digital certificates arranged for authorization purposes as described below, where each successive certificate represents the issuer of the preceding certificate.

A "digital signature" includes digital information signed with a private key of its signatory to ensure that the digital information has not been illicitly modified after being digitally signed. This digital information may be provided in its entirety or as a hash value produced by a one-way hash operation.

A "hash operation" is a one-way conversion of information to a fixed-length representation referred to as a "hash value". Often, the hash value is substantially less in size than the original information. It is contemplated that, in some cases, a 1:1 conversion of the original information may be performed. The term "one-way" indicates that there does not readily exist an inverse function to recover any discernible portion of the original information from the fixed-length hash value. Examples of a hash function include MD5 provided by RSA Data Security of Redwood City, California, or Secure Hash Algorithm (SHA-1) as specified a 1995 publication Secure Hash Standard FIPS 180-1 entitled "Federal Information Processing Standards Publication" (April 17, 1995).

Referring to Figure 1, a block diagram of an illustrative embodiment of a system 100 utilizing the present invention is shown. The system 100 comprises a first platform 110 and a second platform 120. First platform 110 is in communication with second platform 120 via a link 130. A "link" is broadly defined as one or more information-carrying mediums (e.g., electrical wire, optical fiber, cable, bus, or wireless signaling technology). When requested by the

user, first platform 110 generates and transmits a pseudonym public key 140 (described below) to second platform 120. In response, second platform 120 is responsible for certifying, when applicable, that pseudonym public key 140 was generated by a trusted device 150 within first platform 110.

Referring now to Figure 2, in one embodiment, trusted device 150 comprises hardware and/or protected software. Software is deemed "protected" when access control schemes are employed to prevent unauthorized access to any routine or subroutine of the software. More specifically, device 150 is one or more integrated circuits that prevents tampering or snooping from other logic. The integrated circuit(s) may be placed in a single integrated circuit (IC) package or a multi-IC package. A package provides additional protection against tampering. Of course, device 150 could be employed without any IC packaging if additional protection is not desired.

Herein, device 150 comprises a processing unit 200 and a persistent memory 210 (e.g., non-volatile, battery-backed random access memory "RAM", etc.). Processing unit 200 is hardware that is controlled by software that internally processes information. For example, processing unit 200 can perform hash operations, perform logical operations (e.g. multiplication, division, etc.), and/or produce a digital signature by digitally signing information using the Digital Signature Algorithm. Persistent memory 210 contains a unique asymmetric key pair 220 programmed during manufacture. Used for certifying pseudonyms, asymmetric key pair 220 includes a public key (PUKP1) 230 and a private key (PRKP1) 240. Persistent memory 210 may further include a public key 250 (PUKP2) of second platform 120, although it may be placed in volatile memory (e.g., RAM, register set, etc.) within device 150 if applicable.

In this embodiment, device 150 further comprises a number generator 260 such as a random number generator or a pseudo-random number generator. Number generator 260 is responsible for generating a bit stream that is used, at least in part, to produce one or more pseudonyms. A "pseudonym" is an alias identity in the form of an alternate key pair used to establish protected communications with another platform and to identify that its platform includes trusted device 150. The pseudonym also supports a challenge/response protocol and a binding of licensing, secrets and other access control information to the specific platform. It is contemplated, however, that number generator 260 may be employed externally from device 150. In that event, the greater security would be

realized by platform 110 if communications between number generator 260 and device 150 were protected.

Referring to Figure 3, a flowchart of an illustrative embodiment describing allocation and use of a pseudonym is shown. To fully protect the user's privacy, the user should have positive control of the production, allocation and deletion of pseudonyms. Thus, in response to explicit user consent, a new pseudonym is produced (blocks 300 and 310). Also, to access information (e.g., label, public key, etc.) that identifies an existing pseudonym, explicit user consent is needed (blocks 320 and 330). Explicit user consent may be given by supplying a pass-phrase (e.g., series of alphanumeric characters), a token, and/or a biometric characteristic to the trusted device. For example, in one embodiment, a user pass-phrase may be entered through a user input device (e.g., a keyboard, mouse, keypad, joystick, touch pad, track ball, etc.) and transferred to the trusted device. In another embodiment, memory external to the logic may contain pseudonyms encrypted with a hash value of a user pass-phrase. Any of these pseudonyms can be decrypted for use by again supplying the user pass-phrase.

Once a pseudonym has been produced and allocated for use in communications with a remote platform, this pseudonym represents the persistent platform identity for that platform/platform communications, so long as the user chooses to retain the pseudonym (blocks 340, 350 and 360).

Referring now to Figures 4 and 5, flowcharts of an illustrative embodiment of the production and certification of pseudonyms are shown. Initially, upon receiving a request by the user, the pseudonym is produced by the device in coordination with a number (block 400). A pseudonym public key (PPUKP1) is placed in a digital certificate template (block 405). The digital certificate template may be internally stored within the first platform or provided by the second platform in response to a request for certification from the first platform. Thereafter, the digital certificate template undergoes a hash operation to produce a certificate hash value (block 410).

Thereafter, the certificate hash value undergoes a transformation similar to that described in U.S. Patent Nos. 4,759,063 and 4,759,064 to create a "blinded" certificate hash value (block 415). In particular, the certificate hash value is multiplied by a pseudo-random number (e.g., a predetermined number raised to a power that is pseudo-randomly select). The pseudo-random power is maintained in confidence within the first platform (e.g., placed in persistent memory 210 of Figure 2).

A certification request, including at least the transformed (or blinded) certificate hash value, is created (block 420). The certification request is digitally signed with the private key (PRKP1) of the first platform (block 425). A device certificate, namely a digital certificate chain that includes the public key (PUKP1) of the first platform in one embodiment, is retrieved or generated to accompany the signed certificate request (block 430). In this embodiment, the device certificate features a high-level certificate including PUKP1 and a lowest level certificate including the root certificate. Of course, the device certificate may be a single digital certificate including PUKP1. Both the signed certificate request and device certificate are encrypted with the public key (PUKP2) of the second platform and then transferred to the second platform (blocks 435 and 440).

At the second platform, the signed certificate request and device certificate are recovered after being decrypted using the private key (PRKP2) of the second platform (block 445). The public key (PUKP1) of the first platform may be obtained using a public key of the certification authority responsible for signing the device certificate (block 450). If the second platform can recover the certificate request, the second platform verifies the device certificate back to the root certificate (blocks 455 and 460). If the certificate request is recovered and the device certificate is verified, the transformed (or blinded) certificate hash value is digitally signed to produce a "signed result" (block 465). Otherwise, if either the transformed (or blinded) certificate hash value cannot be determined or the device certificate cannot be verified, an error message is returned to the first platform (block 470).

Upon receipt of the signed result from the second platform, the first platform performs an inverse transformation on the signal result. For example, in this illustrative embodiment, the first platform divides the signed result by an inverse of the pseudo-random number (e.g., the predetermined number raised to an inverse of the pseudo-random power) to recover a digital signature of the certificate hash value (blocks 475 and 480). The digital signature is stored with one or more pseudonyms for use in subsequent communications with other platforms to identify that the first platform includes a trusted device.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to

which the invention pertains are deemed to lie within the spirit and scope of the invention.